

## REMARKS

Reconsideration of the above-identified patent application in view of the amendments above and the remarks following is respectfully requested.

Claims 19 and 21-35 are in this case. Claims 19 and 21-35 have been rejected under § 103(a). New claims 36-39 have been added.

The claims before the Examiner are directed toward a method and apparatus for ensuring the integrity of an application executed on a computer. During a learning period, the computer learns the normal access behavior of the application with respect to data storage sectors. Subsequent to the learning period, the computer prohibits or restricts access by the application to the data storage sectors that is inconsistent with the learned normal behavior of the application.

### **§ 103(a) Rejections – Shieh et al. ‘901 in view of Crosbie & Spafford**

The Examiner has rejected claims 19 and 21-35 under § 103(a) as being unpatentable over Shieh et al., US Patent No. 5,278,901 (henceforth, “Shieh et al. ‘901”) in view of Crosbie & Spafford, “Active defense of a computer system using autonomous agents”, *Technical Report No. 95-008*, Department of Computer Science, Purdue University, February 15, 1995 (henceforth, “Crosbie & Spafford”). The Examiner’s rejection is respectfully traversed.

Shieh et al. ‘901 teach a method of detecting hostile intrusions in a computer 104 by, *inter alia*, monitoring file accesses by an application program 102. As Shieh et al. ‘901 state in column 4 lines 52-55,

...as is the case with any model that requires explicit definition of intrusion patterns, the present invention detects only intrusions that can be anticipated prior to their occurrence. (emphasis added)

Crosbie & Spafford propose overcoming this shortcoming using free-running processes that they call “Autonomous Agents”. The Autonomous Agents are trained during a “training phase” to recognize normal and abnormal behavior of the application program. As described on page 6, right-hand column, lines 8-13:

They will be trained to detect anomalous activity in this traffic by being subjected to a training phase by a human operator. The operator will present different styles of network traffic (both intrusive traffic and neutral traffic) and guide the learning of the agents.

The crucial difference between the present invention and the prior art cited by the Examiner is that the prior art cited by the Examiner addresses only the *detection* of abnormal behavior, not the *prevention* or *restriction* of abnormal behavior. Shieh et al. ‘901 are totally silent on the subject of what to do when an intrusion is detected. The only response taught by Crosbie & Spafford (*e.g.* in page 2, left-hand column, line 35 and page 5, right-hand column, line 31) is notifying an operator, not preventing the attempted file access. By contrast, claim 19 recites:

an enforcement device...for identifying and preventing said application from accessing elements of data storage that do not correspond with the normal behavior of said application (emphasis added)

claim 22 recites:

an enforcement device operative...to treat attempts of the program to access files to which the user permitted access during said learning period more leniently than attempts of the program to access files to which the user did not permit access during said learning period (emphasis added)

claim 24 recites:

an enforcement device operative...to treat attempts of the program to access files accessed during said learning period more leniently than attempts of the program to access files not accessed during said learning period... (emphasis added)

and claim 25 recites:

...detecting attempts of said application to access elements of data storage that do not correspond to said normal behavior...and inhibiting said accesses... (emphasis added)

Thus, independent claims 19, 22, 24 and 25 are allowable in their present form. It follows that claims 21, 23, and 26-35, that depend therefrom, also are allowable.

### New Claims

New claims 36-39 have been added. New claims 36-39 add to claims 19, 22, 24 and 25, respectively, the limitation that during the learning period, the computer learns only the normal behavior of the application. This aspect of the present invention is stated on page 9 lines 11-17, as amended as described below:

In the event that an enforcement file is not available, an embodiment of the invention, whose flow diagram is shown in Figure 2, has a so-called learn mode 21. In this mode a new program is assigned a general enforcement file. The general enforcement file gives the program no access rights at all to files on the system disk. The program then attempts to make a file access 20. Provided the attempt is within certain parameters the system allows the attempt and learns the details 23 so that in future an access to that area of the disk will always be allowed. Thus a specific enforcement file is gradually built up over the duration of the learn mode. (emphasis added)

In other words, it is assumed that all the memory accesses by the application during the learning period are normal memory accesses, and only the details of these normal memory accesses are recorded. This is in contrast to the teachings of Crosbie & Spafford, who explicitly present their Autonomous Agents with both “intrusive traffic” and “neutral traffic”.

### Objections to the Drawings

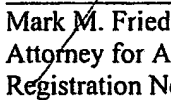
The Examiner has objected to the drawings for not showing the learning period. Attached please find a replacement sheet for Figures 1 and 2 in which steps

21 and 23 have been added to describe the learning period. (Figure 2 as filed illustrated the second embodiment of the present invention only subsequent to the learning mode.) The paragraph beginning on page 9 line 11 has been amended to refer to steps 21 and 23. No new matter has been added.

The Examiner has objected to a spelling error in step 38 of Figure 3. Attached please find a replacement sheet for Figures 3 and 4 with this spelling error corrected.

In view of the above amendments and remarks it is respectfully submitted that independent claims 19, 22, 24 and 25, and hence dependent claims 21, 23 and 26-39 are in condition for allowance. Prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,



---

Mark M. Friedman  
Attorney for Applicant  
Registration No. 33,883

Date: August 25, 2004